UNITED STATES DISTRICT COURT

for the

Eastern District of California

In the Matter of the Search of

INFORMATION ASSOCIATED WITH KIK ACCOUNT "HAVEYOUDRIPPIN69" THAT IS STORED AT PREMISES CONTROLLED BY MEDIALAB.AI INC.

Case No. 2:23-sw-0593 CKD

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

SEE ATTACHMENT A, attached hereto and incorporated by reference.

located in the Central District of California, there is now concealed *(identify the person or describe the property to be seized)*:

SEE ATTACHMENT B, attached hereto and incorporated by reference

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☐ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. § 2252(a)(2)	Receipt or Distribution of Child Pornography
18 U.S.C. § 2252(a)(4)(B)	Possession of Child Pornography

The application is based on these facts:

SEE AFFIDAVIT, attached hereto and incorporated by reference.

- ☑ Continued on the attached sheet.
- ☐ Delayed notice 30 days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

/s/
Applicant's signature

HSI Special Agent Casey Snyder
Printed name and title

Sworn to me and signed telephonically.

Date: June 14, 2023 at 4:04 pm

Carolyn K. Delaney
Judge's signature

City and state: Sacramento, California

Carolyn K. Delaney, U.S. Magistrate Judge
Printed name and title

AFFIDAVIT OF CASEY SNYDER IN SUPPORT OF SEARCH WARRANT APPLICATION

I, Casey Snyder, a Special Agent with the U.S. Department of Homeland Security, Homeland Security Investigations ("HSI") being first duly sworn, hereby depose and state as follows:

I. INTRODUCTION AND AGENT BACKGROUND

1. I am a Special Agent with Homeland Security Investigations and have been since June 2022. Prior to HSI, I was a Special Agent with the U.S. Postal Service, Office of Inspector General for over ten years. I received my initial training at the Federal Law Enforcement Training Center in Glynco, Georgia, in 2008. Most recently, I completed the HSI Special Agent Training (HSISAT) course at FLETC in December of 2022. While employed by HSI, I have investigated federal criminal violations related to high technology or cybercrime, child exploitation, and child pornography. I have gained experience by successfully completing the Criminal Investigator Training Program (CITP) at the Federal Law Enforcement Training Center (FLETC) in Glynco, Georgia, the HSISAT program at FLETC in Glynco, Georgia, advanced training, and everyday work relating to conducting these types of investigations. In the course of my employment, I have served or assisted in serving search warrants; seized numerous items of computer equipment and digital evidence; and I have participated in several investigations involving computer forensics, including investigations related to child pornography and exploitation. I have received training in the area of child pornography and child exploitation. I have also had the opportunity to observe and review numerous examples of child pornography (as defined in 18 U.S.C. § 2256(8)) in all forms of media including computer media. I have been a Special Agent for over fourteen (14) years and am a federal law enforcement officer who is engaged in enforcing criminal laws, including 18 U.S.C. §§ 2251, 2252, and 2252A, and I am authorized by law to request a search warrant.

2. Kik is an instant messaging application available on mobile phones that allows its users to send videos and still images to other Kik users. Kik is operated by MediaLab.ai Inc.

("MediaLab"), a social networking company headquartered in Santa Monica, California.

3. I make this affidavit in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A), and 2703(c)(1)(A) to require MediaLab to disclose to the government records and other information in its possession pertaining to the subscriber or customer associated with the Kik username "haveyoudrippin69" ("**TARGET ACCOUNT**"). The information to be searched is described in the following paragraphs and in Attachments A and B. Attachments A and B are incorporated in this affidavit by reference.

4. This affidavit is submitted in connection with an investigation into the receipt, distribution, and possession of Child Sexual Assault Material (CSAM) via Kik by Jacob BESS, who resides at 1464 Live Oak Boulevard, Yuba City, California 95991.

5. As set forth below, probable cause exists to believe that violations of 18 U.S.C. § 2252(a)(2) (receipt or distribution of child pornography) and 18 U.S.C. § 2252(a)(4)(B) (possession of child pornography) have occurred, that the violations involved the **TARGET ACCOUNT**, and that evidence, contraband, fruits, and instrumentalities of those violations are likely to be found within the **TARGET ACCOUNT**.

6. I am familiar with the information contained in this affidavit based upon the investigation I have conducted, my training and experience, and information provided to me by other law enforcement officers who have engaged in investigations involving the receipt and distribution of CSAM through instant messaging applications installed on mobile phones and other electronic devices. Because this Affidavit is submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation.

II. DEFINITIONS

7. The following definitions apply to this Affidavit and Attachments A and B:

a. Child Pornography," as defined in 18 U.S.C. § 2256(8), and "Child Sexual Assault Material" ("CSAM") mean any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture, whether made or produced by electronic, mechanical, or other means, of sexually explicit conduct where (a) the production of such visual depiction involved the use of a minor engaged in sexually explicit conduct; (b) such visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct; or (c) such visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct. Where possible, your affiant has used "CSAM" in place of "child pornography" throughout this application. All references to "CSAM" in this application reference child pornography as defined in 18 U.S.C. § 2256(8).

b. A "Computer," as defined in 18 U.S.C. § 1030(e)(1), means "an electronic, magnetic, optical, electrochemical, or other high-speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device."

c. "Internet Protocol address" or "IP address" means a unique number used by a computer to access the Internet. IP addresses can be dynamic, which means that the Internet Service Provider ("ISP") assigns a different unique number to a computer every time it accesses the Internet. IP addresses might also be static, which means that the ISP assigned a user's computer a particular IP address that is used each time the computer accesses the Internet.

d. A "Minor," as defined in 18 U.S.C. § 2256(1), means any person under the age of eighteen years.

e. "Sexually explicit conduct," within the meaning of 18 U.S.C. § 2256(2)(A), means actual or simulated (a) sexual intercourse, including genital-genital,

oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic areas of any person.

f. "Visual depictions," within the meaning of 18 U.S.C. § 2256(5), means undeveloped film and videotape, data stored on computer disk or by electronic means which is capable of conversion into a visual image, and data which is capable of conversion into a visual image that has been transmitted by any means, whether or not stored in a permanent format.

g. The terms "Records," "Documents," and "Materials" means all information recorded in any form.

h. "Hash value" refers to a cryptographic algorithm generated against data to produce a numeric value that is representative of that data. They are often referred to as the unique, tamper-evident digital signature or fingerprints for computer files. The most commonly used algorithms are known as message-digest algorithm (MD5) and secure hash algorithm (SHA).

i. "Peer-to-peer" refers to a file sharing network where digital computer files are made available to other computers for download over the internet. People who join a peer-to-peer file sharing network may download copies of files from other users without relying on a dedicated central server.

j. "Android ID" refers to a 64-bit number, expressed as a hexadecimal string, that is unique to a combination of app-signing key, user, and device that is using the Android operating system.

On Android 8.0 and higher versions of the operating system, the number may change if a factory reset is performed on the device.

III. BACKGROUND ON COMPUTERS AND CSAM

8. Based on my knowledge, training, and experience in child exploitation and CSAM investigations, and the experience and training of other law enforcement officers with

whom I have spoken, I know that computers, computer technology, and the internet are critical components in the production, distribution, and collection of CSAM.

9. A CSAM image or video taken with a digital camera or mobile phone can be transferred directly to a computer, and then transferred from that computer to any other server or computer connected to the internet via modem or wireless connection. Many devices not traditionally thought of as computers, such as video game consoles, smartphones, and digital media players likewise have the ability to store digital data, access the internet, and send or receive digital data electronically.

10. CSAM collectors may use online resources to retrieve and store exploitation material, including services offered by internet portals such as Yahoo! and Google, Microsoft OneDrive, Dropbox, MEGA.co.nz, as well as social media applications such as Kik Messenger, among others. The online resources allow a user to set up an account with a remote computing service that provides e-mail services as well as electronic storage of computer files in a variety of formats. A user can set up an online storage account from any computer with access to the Internet. Evidence of online storage of CSAM is often found on the user's computer.

11. Communications made to or from a computer are often saved or stored on that computer. Storing this information can be intentional. For example, a user can save an e-mail as a file on the computer. Digital information can also be retained unintentionally. Traces of the path of an electronic communication may be automatically stored in many places such as temporary "cache" folders. In addition to electronic communications, a computer user's Internet activities generally leave traces in a computer's web cache and Internet history files. A forensic examiner often can recover evidence that shows whether a computer contains peer-to-peer software, whether the computer was sharing files, the extent a user traded images or videos through a social media application, the contents of certain files that were uploaded or downloaded, and whether certain files were deleted.

12. Computer files or remnants of such files can be recovered years after they were viewed, downloaded, or deleted. Deleted files can often be recovered months or years later using

readily available forensic tools. This recovery is possible because a deleted file does not actually disappear. Rather, it remains on the computer's hard drive until it is overwritten by new data. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file. Files that have been viewed via the Internet are automatically downloaded into a temporary Internet directory or "cache." The browser typically maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages. Thus, the ability to retrieve residue of an electronic file from a hard drive depends less on when the file was downloaded or viewed than on a particular user's operating system, storage capacity, and computer habits.

IV. BACKGROUND ON KIK MESSENGER

13. Kik is operated by MediaLab, a social networking company headquartered in Santa Monica, California. In October 2019, Kik was purchased by MediaLab, a company operating in the United States. Kik is a messaging application that is used on smartphones. It advertises itself as "the first smartphone messenger with a built-in browser." Kik users can send messages to other Kik users and share images and videos with each other.

14. Unlike other messengers, Kik usernames – not phone numbers – are the basis for Kik user accounts. This feature helps Kik users maintain a private and anonymous presence on the platform.

15. Kik is widely available for download onto devices that run the iOS operating system (such as iPhones) or the Android operating system. In addition to smart phones, Kik can be downloaded onto tablets such as iPads.

16. In general, MediaLab asks each Kik subscriber to provided certain personal identifying information when registering for an account. This information includes the subscriber's first and last name (which the subscriber can select and change at any time), username, birthday, valid email address, and password. Subscribers also have the option to add a phone number to the account.

17. MediaLab typically retains certain transactional information about the creation

and use of each Kik account. This information can include account creation data, device-related information, the length of service, records of log-in (i.e., session) times, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account, and other log files that reflect usage of the account. In addition, MediaLab often maintains records of the IP address used to register the account and the IP adaddresses associated with the particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the account. Kik also maintains content data, including images and videos exchanged via Kik messages.

18. Kik offers users the ability to create an identity within Kik referred to as a "username." This username is unique to the account and cannot be changed. No one else can utilize the same username. A Kik user would have to create a new account in order to obtain a different username. The username for a particular Kik account holder is generally displayed in their Kik profile.

V. FACTS SUPPORTING PROBABLE CAUSE

19. On May 25, 2023, while conducting an undercover chat operation, an HSI Detroit Special Agent (SA) acted in an undercover capacity portraying himself as the father of an 8-year-old girl on the Kik platform. That same day, Kik user "haveyoudrippin69," (the **TARGET ACCOUNT**) later identified as Jacob BESS of Yuba City, California; sent the HSI SA a private message claiming that he had a 7-year-old daughter. The conversation quickly escalated into sexualized conversation surrounding BESS' daughter. This information was ultimately passed onto to HSI Sacramento for investigation.

20. On May 25, 2023, HSI Sacramento reviewed a screen recording of the Kik conversation as well as the images sent by BESS**.** The following is a description of the review of the conversation between the HSI SA and BESS**:**

BESS began the conversation on Kik by stating that "[he has] a 7yo daughter." The HSI

Special Agent acting in an undercover capacity (hereinafter referred to as Undercover Agent, "UCA") inquired whether she was "active;" to which he responded, "she likes to grind on my dick. She's not used to the taste of cum just yet but she's getting there." The UCA then asked whether he puts "it in her mouth" and if she "swallow[s]." BESS responded that she does but she "gags" and that he "just love[s] how curious she is."

BESS later sent an image of what appears to be a prepubescent female wearing a pink swimsuit bottom and rainbow swimsuit top about to jump into a pool; BESS commented underneath this photo, "Lexi."[1]

The UCA then inquired if BESS took "any dirty pics?" to which BESS responded "Yeah, you?" and sent an image. A description of this image is as follows:

> A color image depicting a prepubescent minor female wearing what appears to be a pink top and nude from the waist down. The image appears to have been taken from below looking upwards at the minor female's vagina. There is no visible pubic hair.

The UCA then inquired if BESS took "any vid of [him] and her." BESS responded again with, "Yeah, you?" BESS sent a video shortly thereafter; a description of this file is as follows:

> This video, approximately 24 seconds in length, is a close-up of what appears to be a vagina of a prepubescent female due to lack of pubic hair. An adult hand is used to spread the buttocks apart, the camera is brought closer to the opening of

[1] Based on the investigation thus far, law enforcement confirmed BESS has a 10-year-old daughter named Lexi. Law enforcement also learned BESS has a seven-year-old daughter.

the vagina. A finger is then placed around the vagina and slides up towards the anus and back down towards the vagina."

When the UCA inquired when that last was, BESS responded, "not long ago, let me see your baby." The UCA later asked whether there were any videos taken of BESS "in her mouth??" BESS responded with "I'll see if I can get her to right now [smiling emoji with tongue sticking out]" The UCA asked BESS if he was with her right now to which he responded "Yep."

When asked where BESS has anything saved, he responded that he doesn't "on [his] phone" but that "she has stuff on her tablet though." When asked what kind of stuff, BESS stated that "she's always dancing naked, masturbating, sucking on toys, and playing with her moms dildo."

During the conversation, BESS informed the UCA that he has his daughter "on [his] lap right now."

When asked whether BESS was near Michigan, he stated that he is in California.

At one point in the conversation, the UCA inquired what BESS looks like. It appeared he initially misread the question and stated, "little girls lol." BESS followed up this statement with the following messages:

"Oh lol I read that wrong"

"I thought you asked 'what do you like'"

When asked what was the most he's done with his daughter, BESS stated that he thinks they've "done it all lol." He followed up with the following message:

"She just likes me eating her pussy and rubbing my dick on it until I cum inside her"

21. Following this conversation, the HSI UCA sent an emergency disclosure request to Kik for subscriber information for BESS. Kik responded with a first name "Jakoby," Last name "Tress," email address "diggem77@gmail.com," and the **TARGET ACCOUNT**. Per Kik, the IP address 73.66.232.56 was associated with the **TARGET ACCOUNT** on several occasions.

22. HSI contacted Comcast Cable for emergency disclosure of subscriber information for the IP address 73.66.232.56. Comcast verbally provided the subscriber associated with the IP address as: Justine Chesser, 530-755-7384, 1464 Live Oak Blvd, Yuba City, CA 95991. Law enforcement records showed the phone number 530-755-7384 was associated to both Chesser and BESS.

23. HSI reviewed law enforcement records for calls for service associated with the SUBJECT PREMISES. The records showed multiple calls for service by law enforcement between December 2022 and January 2023. On January 3, 2023, Yuba City Police Department responded to the SUBJECT PREMISES for a child custody incident involving BESS. The Yuba City Police Department again responded to the SUBJECT PREMISES on January 13, 2023, for a child custody incident involving BESS. During this incident, BESS contacted police and stated his son was with him at the SUBJECT PREMISES. On January 14, 2023, Yuba County Police Department responded to the SUBJECT PREMISES to check on two minors, one of which was named "LEXI".

24. Based on the above information, HSI Sacramento applied for a search warrant to search BESS and his residence, located at 1464 Live Oak Blvd, Yuba City, CA 95991. The Honorable Judge Jeremy D. Peterson authorized the search warrant on May 25, 2023 (Case No. 2:23-SW-0519 JDP).

25. Prior to executing the search warrant, law enforcement submitted a preservation

request to MediaLab for the **TARGET ACCOUNT**.

26. Law enforcement executed the search warrant at the residence on May 25, 2023. BESS was not on the premises when law enforcement began executing the warrant, but arrived shortly thereafter. BESS arrived alone, driving his personal vehicle. When BESS arrived, he was placed into custody by Yuba City Police Department, Yuba City, CA. He was later booked into state custody on state child pornography charges. Law enforcement located BESS' cell phone, in the passenger seat of the vehicle and seized the cell phone. The cell phone was seized from the immediate area of where BESS had been sitting when he drove his vehicle home.

27. On May 25, 2023, law enforcement interviewed BESS. After being advised of his Miranda Rights, BESS admitted to chatting and sending child pornography while using the **TARGET ACCOUNT** on May 25, 2023. BESS further admitted to regularly receiving, possessing, and distributing what he knew to be child pornography. BESS stated he only used his cellular phone to use chatting applications, such as Kik, and to receive or send child pornography. BESS described his cell phone as the cell phone found in the passenger seat of his vehicle when he arrived at his residence.

VI. CONCLUSION

28. Based on the aforementioned factual information, there is probable cause to believe that BESS possessed, received, and distributed child sexual abuse material, in violation of 18 U.S.C. §§ 2252(a)(2) and 2252(a)(4)(B); and that he did so using the **TARGET ACCOUNT**. Thus, I request a search warrant requiring MediaLab, an electronic communications service provider, to provide contents of electronic communications and electronic files pertaining to the **TARGET ACCOUNT**, Kik username haveyoudrippin69, and request that the Court issue the proposed search warrant authorizing the search of the account described in Attachment A for the items described in Attachment B.

///

///

///

29. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant. The government will execute this warrant by serving it electronically on MediaLab. MediaLab will then compile the requested records at a time convenient to it. Thus, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

Respectfully submitted,

/s/

Casey Snyder
Special Agent
Homeland Security Investigations

Subscribed and sworn to me telephonically on:
June 14, 2023 at 4:04 pm

Hon. Carolyn K. Delaney
U.S. MAGISTRATE JUDGE

/s/ *Emily G. Sauvageau*
Approved as to form by AUSA EMILY G. SAUVAGEAU

ATTACHMENT A

This warrant applies to information associated with Kik Account "haveyoudrippin69" that is stored at the premises owned, maintained, controlled, or operated by Medialab.ai Inc., a company headquartered at 1237 7th Street, Santa Monica, CA 90401.

ATTACHMENT B

ITEMS TO BE SEIZED

Items constituting evidence, contraband, fruits, or instrumentalities of violations of 18 U.S.C. §§ 2252(a)(2) and 2252(a)(4)(B), as follows:

I. INFORMATION TO BE DISCLOSED BY THE PROVIDER

To the extent that the information described in Attachment A is within the possession, custody, or control of MEDIALAB.AI INC. ("the Provider"), including any information that has been deleted but is still available to the Provider, or has been preserved pursuant to the request made under 18 U.S.C. § 2703(f) on May 25, 2023, the Provider is required to disclose the following information to the government for the account listed in Attachment A:

1. IP addresses associated to the Kik account **haveyoudrippin69**;
2. All transactional chat logs associated to the Kik account **haveyoudrippin69**;
3. The content of all messages associated to the Kik account **haveyoudrippin69**;
4. All images and video associated to the Kik account **haveyoudrippin69** including the unknown usernames and IP address associated to the sender of images and videos;
5. A date-stamped log showing the usernames that Kik account **haveyoudrippin69** added and/or blocked;
6. All abuse reports associated to the Kik account **haveyoudrippin69**;
7. All emails associated to the Kik account **haveyoudrippin69**;
8. Registration IP address associated to the Kik account **haveyoudrippin69**; and,
9. All other information relevant to the account held by MediaLab.ai Inc.

The Provider is hereby ordered to disclose the above information to the government within 14 days of issuance of this warrant.

II. INFORMATION TO BE SEIZED BY THE GOVERNMENT

All information described above in Section I of this attachment that constitutes fruits, contraband, evidence, and instrumentalities of violations of 18 U.S.C. §§ 2252(a)(2) and 2252(a)(4)(B), that involve Kik accounts "**haveyoudrippin69**," Jacob BESS, aka Jakoby TRESS, the IP address 73.66.232.56, or the email address "diggem77@gmail.com", including information pertaining to the following matters:

1. The production of child pornography;
2. The receipt of child pornography;
3. The possession of child pornography;
4. Information relating to who created, used, or communicated with the "**haveyoudrippin69**" Kik account, including records about their identities and whereabouts;
5. Indica of who used, accessed, controlled, or created the Kik account "**haveyoudrippin69**."

UNITED STATES DISTRICT COURT

for the

Eastern District of California

In the Matter of the Search of INFORMATION ASSOCIATED WITH KIK ACCOUNT "HAVEYOUDRIPPIN69" THAT IS STORED AT PREMISES CONTROLLED BY MEDIALAB.AI INC.	)	Case No. 2:23-sw-0593 CKD

SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search of the following person or property located in the Central District of California *(identify the person or describe the property to be searched and give its location)*:

SEE ATTACHMENT A, attached hereto and incorporated by reference.

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal *(identify the person or describe the property to be seized)*:

SEE ATTACHMENT B, attached hereto and incorporated by reference.

YOU ARE COMMANDED to execute this warrant on or before June 27, 2023 *(not to exceed 14 days)*

☐ in the daytime 6:00 a.m. to 10:00 p.m. ☑ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to: any authorized U.S. Magistrate Judge in the Eastern District of California.

☐ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized *(check the appropriate box)*

☐ for 30 days *(not to exceed 30)* ☐ until, the facts justifying, the later specific date of _____.

Date and time issued: June 14, 2023 at 4:04 pm

Carolyn K. Delaney
Judge's signature

City and state: Sacramento, California

Carolyn K. Delaney, U.S. Magistrate Judge
Printed name and title

AO 93 (Rev. 11/13) Search and Seizure Warrant (Page 2) (modified)

Return		
Case No.:	Date and time warrant executed:	Copy of warrant and inventory left with:
Inventory made in the presence of :		
Inventory of the property taken and name of any person(s) seized:		

Certification

I swear that this inventory is a true and detailed account of the person or property taken by me on the warrant.

Subscribed, sworn to, and returned before me this date.

Signature of Judge

Date

ATTACHMENT A

This warrant applies to information associated with Kik Account "haveyoudrippin69" that is stored at the premises owned, maintained, controlled, or operated by Medialab.ai Inc., a company headquartered at 1237 7th Street, Santa Monica, CA 90401.

ATTACHMENT B

ITEMS TO BE SEIZED

Items constituting evidence, contraband, fruits, or instrumentalities of violations of 18 U.S.C. §§ 2252(a)(2) and 2252(a)(4)(B), as follows:

I. INFORMATION TO BE DISCLOSED BY THE PROVIDER

To the extent that the information described in Attachment A is within the possession, custody, or control of MEDIALAB.AI INC. ("the Provider"), including any information that has been deleted but is still available to the Provider, or has been preserved pursuant to the request made under 18 U.S.C. § 2703(f) on May 25, 2023, the Provider is required to disclose the following information to the government for the account listed in Attachment A:

1. IP addresses associated to the Kik account **haveyoudrippin69**;
2. All transactional chat logs associated to the Kik account **haveyoudrippin69**;
3. The content of all messages associated to the Kik account **haveyoudrippin69**;
4. All images and video associated to the Kik account **haveyoudrippin69** including the unknown usernames and IP address associated to the sender of images and videos;
5. A date-stamped log showing the usernames that Kik account **haveyoudrippin69** added and/or blocked;
6. All abuse reports associated to the Kik account **haveyoudrippin69**;
7. All emails associated to the Kik account **haveyoudrippin69**;
8. Registration IP address associated to the Kik account **haveyoudrippin69**; and,
9. All other information relevant to the account held by MediaLab.ai Inc.

The Provider is hereby ordered to disclose the above information to the government within 14 days of issuance of this warrant.

II. INFORMATION TO BE SEIZED BY THE GOVERNMENT

All information described above in Section I of this attachment that constitutes fruits, contraband, evidence, and instrumentalities of violations of 18 U.S.C. §§ 2252(a)(2) and 2252(a)(4)(B), that involve Kik accounts "**haveyoudrippin69**," Jacob BESS, aka Jakoby TRESS, the IP address 73.66.232.56, or the email address "diggem77@gmail.com", including information pertaining to the following matters:

1. The production of child pornography;
2. The receipt of child pornography;
3. The possession of child pornography;
4. Information relating to who created, used, or communicated with the "**haveyoudrippin69**" Kik account, including records about their identities and whereabouts;
5. Indica of who used, accessed, controlled, or created the Kik account "**haveyoudrippin69**."